ABSTRACT OF THE DISCLOSURE

An object is to evaluate the strength in consideration of the relationship held between keys, to allow the detection of a weak key condition to lower the difficulty in decrypting ciphertext, and to detect a weak key based on the weak key condition. Based on the relationship between keys in a key schedule and based on estimated keys, a certain estimated extended key can be calculated by utilizing the relationship between the estimated extended key in the key schedule and an estimated extended key having been calculated, and cost information required for calculation is outputted to allow the verification of a weak key condition. A weak key can be detected based on the weak key condition, and the difficulty in decrypting ciphertext can be increased without modifying an encryption apparatus.